| REPORT DOCUMENTATION PAGE | *Form Approved OMB No. 0704-0188* |
|---|---|



**1. REPORT DATE** *(DD-MM-YYYY)*: 01-14-2008

**2. REPORT TYPE**: Final Report

**3. DATES COVERED** *(From - To)*: 15-JUL-2004 through 31-DEC-2006

**4. TITLE AND SUBTITLE**

Distributed System Security via Logical Frameworks (SeLF)

**5a. CONTRACT NUMBER**: N000140410724

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**6. AUTHOR(S)**

PI's: Lujo Bauer, Frank Pfenning, Michael Reiter

Researchers: Kaustav Chaudhuri, Deepak Garg, Scott Garriss, Jon McCune, Jason Rouse, Kevin Watkins

Collaborators: Ruy Ley-Wild, Pablo Lopez, Jeff Polakow

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Carnegie Mellon University
Computer Science Department
5000 Forbes Avenue
Pittsburgh, PA 15213

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Ralph F. Wachter
Office of Naval Research
875 North Randolph Street
Arlington, VA 22203-1995

**10. SPONSOR/MONITOR'S ACRONYM(S)**: ONR

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

http://www.cs.cmu.edu/~self/
Approved for public release; distribution is Unlimited

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

Please see attached document titled:

Distributed System Security via Logical Frameworks
ONR N00014-04-1-0724
Final Report

**15. SUBJECT TERMS**

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | 19b. TELEPHONE NUMBER *(Include area code)* |
| | | | | | |

## INSTRUCTIONS FOR COMPLETING SF 298

**1. REPORT DATE.** Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

**2. REPORT TYPE.** State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

**3. DATES COVERED.** Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

**4. TITLE.** Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

**5a. CONTRACT NUMBER.** Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

**5b. GRANT NUMBER.** Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

**5c. PROGRAM ELEMENT NUMBER.** Enter all program element numbers as they appear in the report, e.g. 61101A.

**5d. PROJECT NUMBER.** Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

**5e. TASK NUMBER.** Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

**5f. WORK UNIT NUMBER.** Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

**6. AUTHOR(S).** Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES).** Self-explanatory.

**8. PERFORMING ORGANIZATION REPORT NUMBER.** Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES).** Enter the name and address of the organization(s) financially responsible for and monitoring the work.

**10. SPONSOR/MONITOR'S ACRONYM(S).** Enter, if available, e.g. BRL, ARDEC, NADC.

**11. SPONSOR/MONITOR'S REPORT NUMBER(S).** Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

**12. DISTRIBUTION/AVAILABILITY STATEMENT.** Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

**13. SUPPLEMENTARY NOTES.** Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

**14. ABSTRACT.** A brief (approximately 200 words) factual summary of the most significant information.

**15. SUBJECT TERMS.** Key words or phrases identifying major concepts in the report.

**16. SECURITY CLASSIFICATION.** Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

**17. LIMITATION OF ABSTRACT.** This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

# Distributed System Security via Logical Frameworks

ONR N00014-04-1-0724
Final Report

Frank Pfenning, Carnegie Mellon University

Michael Reiter, Carnegie Mellon University
Lujo Bauer, Carnegie Mellon University

## 1 Objectives and Approach

We conducted a research program with the goal of advancing security in distributed systems via the application of logical frameworks. Our work targeted multiple facets of the life-cycle of a distributed system, ranging from design through execution, and from sound mechanism design through sound policy enforcement. It consisted of three major interconnected thrusts.

First, we investigated how to exploit existing technologies to mechanically reason about security policies as specified in a logical framework. This closed an important security gap, helping users and managers understand the consequences of their policies.

Second, we demonstrated the use of logical frameworks for encoding and enforcing access-control policies in a practical distributed system. Access-control mechanisms today, whether it be physical keys for doors or password protection for computer accounts, reflect access-control policies that are explicit only in the manual procedures of the organization that manages these resources. As such, any change in policy, e.g., creating a new computer account, or permitting a person to unlock a door, is effected through a manual process. We utilized logical frameworks to encode organizational policies within computer systems, thereby harnessing the power of these frameworks to support the management and enforcement of access-control policy, and gaining security and flexibility by doing so. We demonstrated this capability in a ubiquitous computing test-bed at Carnegie Mellon.

Third, we developed and implemented a framework for the specification of distributed and concurrent systems and their implementations, specifically targeting our test-bad architecture. This work extends a previous collaboration between NRL and Carnegie Mellon that resulted in the design of CLF, an innovative logical language for the specification of concurrent systems. CLF incorporates ideas from logical frameworks, linear logic, and monads into an expressive meta-language.

Prior work was supported by the Office of Naval Research (ONR) Grant N00173-00-C-2086 – *Efficient Logics for Reasoning about Security Protocols and Their Implementations.* CLF is now fully specified and has been successfully validated on mainstream concurrency formalisms (e.g., Petri nets, the pi-calculus), advanced concurrent programming languages (Concurrent ML), and security protocol specification languages (MSR). In the context of the present contract, we facilitated the transition of CLF from a foundational language into an implemented tool that can be applied to the specification of complex distributed and concurrent systems through the LolliMon prototype.

## 2 Technical Accomplishments

The research carried out under this grant accomplished the stated objectives. We will line them up with the threads of inquiry listed above. An overview of the project and accomplishments in the middle of the grant period can be found in [BPR07].

**Reasoning about security policies.** In an invited workshop talk [Pfe05] we mapped out a constructive logic for specifying security properties of distributed systems. We analyzed its properties and developed several criteria to establish noninterference between principals in [GP06]. In an approach to security based on formal logics and their proofs, this is a critical component.

**Practical implementation.** We implemented our designs as part of the Grey system for universal access control via convergent devices [BGM+05]. This system is currently in use on the Cylab floor of the Collaborative Innovation Center at Carnegie Mellon University, where students, faculty, and staff use smart phones to control access to their offices and log into their computers.

The experience with this implementation led to several further developments on the logical side. Specifically, we considered linear extensions to handle consumable (use-once) certificates [BBG+07] as well as an explicit representation of the knowledge of principles [GBB+06]. These advances were only partially implemented during the course of the contract, but make important conceptual contributions.

A crucial aspect of the practical implementation side is proof search, because access to a resource is granted when a formal proof of compliance with the access control policy is presented. For the Grey system this was solved through a distributed backward-chaining proof search engine [BGR05].

For extensions with consumable resources, we developed a separate, stand-alone theorem prover for linear logic [CP05a, Cha06]. Further development of this prover required a number of fundamental advances in our understanding of proof search for linear logic [CP05b, CPP06]. All these insights are integrated into our distributed software.

**Specifications for Concurrent Systems.** The focus in this thread was the development of an operational semantics so as to simulate the distributed systems specified in the Concurrent Logical Framework (CLF). In order to make this feasible, we restricted ourselves to a large fragment of CLF that is sufficient to express much of the proof-carrying authorization architecture of Grey. The design of this language [LPPW05] is a significant result of the work under this grant. The implementation is complete and publicly available.

A sideline was the analysis of causal dependencies in a logical framework, at present published only as a technical report [LWP07].

# 3 References

## References

[BBG+07] Kevin D. Bowers, Lujo Bauer, Deepak Garg, Frank Pfenning, and Michael K. Reiter. Consumable credentials in logic-based access-control systems. In *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS'07)*, pages 143–157, San Diego, California, February 2007. Internet Society. Preliminary version available as Technical Report CMU-CYLAB-06-002, Carnegie Mellon University, February 2006.

[BGM+05] Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, and Peter Rutenbar. Device-enabled authorization in the Grey system. In *Proceedings of the 8th Information Security Conference (ISC'05)*, pages 431–445, Singapore, September

2005. Springer Verlag LNCS 3650. Reprinted in: *Information Security Research: New Methods for Protecting Against Cyber Threats*, pp. 116–130, Department of Defense, Wiley Publishing, 2007.

[BGR05] Lujo Bauer, Scott Garriss, and Michael K. Reiter. Distributed proving in access-control systems. In V.Paxon and M.Waidner, editors, *Proceedings of the 2005 Symposium on Security and Privacy (S&P'05)*, pages 81–95, Oakland, California, May 2005. IEEE Computer Society Press.

[BPR07] Lujo Bauer, Frank Pfenning, and Michael K. Reiter. Distributed system security via logical frameworks. In *Information Security Research: New Methods for Protecting Against Cyber Threats*, pages 108–115. Department of Defense, Wiley Publishing, 2007.

[Cha06] Kaustuv Chaudhuri. *The Focused Inverse Method for Linear Logic.* PhD thesis, Carnegie Mellon University, December 2006. Available as technical report CMU-CS-06-162.

[CP05a] Kaustuv Chaudhuri and Frank Pfenning. A focusing inverse method prover for first-order linear logic. In R.Nieuwenhuis, editor, *Proceedings of the 20th International Conference on Automated Deduction (CADE-20)*, pages 69–83, Tallinn, Estonia, July 2005. Springer Verlag LNCS 3632.

[CP05b] Kaustuv Chaudhuri and Frank Pfenning. Focusing the inverse method for linear logic. In L.Ong, editor, *Proceedings of the 14th Annual Conference on Computer Science Logic (CSL'05)*, pages 200–215, Oxford, England, August 2005. Springer Verlag LNCS 3634.

[CPP06] Kaustuv Chaudhuri, Frank Pfenning, and Greg Price. A logical characterization of forward and backward chaining in the inverse method. In U. Furbach and N. Shankar, editors, *Proceedings of the 3rd International Joint Conference on Automated Reasoning (IJCAR'06)*, pages 97–111, Seattle, Washington, August 2006. Springer LNCS 4130. Extended and revised version to appear in a special issue of the Journal of Automated Reasoning with selected papers from IJCAR 2006.

[GBB+06] Deepak Garg, Lujo Bauer, Kevin Bowers, Frank Pfenning, and Michael Reiter. A linear logic of affirmation and knowledge. In D. Gollman, J. Meier, and A. Sabelfeld, editors, *Proceedings of the 11th European Symposium on Research in Computer Security (ESORICS'06)*, pages 297–312, Hamburg, Germany, September 2006. Springer LNCS 4189.

[GP06] Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In J. Guttman, editor, *Proceedings of the 19th Computer Security Foundations Workshop (CSFW'06)*, pages 283–293, Venice, Italy, July 2006. IEEE Computer Society Press.

[LPPW05] Pablo López, Frank Pfenning, Jeff Polakow, and Kevin Watkins. Monadic concurrent linear logic programming. In A.Felty, editor, *Proceedings of the 7th International Symposium on Principles and Practice of Declarative Programming (PPDP'05)*, pages 35–46, Lisbon, Portugal, July 2005. ACM Press.

[LWP07] Ruy Ley-Wild and Frank Pfenning. Avoiding causal dependencies via proof irrelevance in a concurrent logical framework. Technical Report CMU-CS-07-107, Carnegie Mellon University, February 2007.

[Pfe05] Frank Pfenning. Constructive authorization logics. Invited talk at the 4th Workshop on Foundations of Computer Security (FCS'05), July 2005.

## 4 Software Prototypes

We are distributing two software prototypes developed with funds from this grant.

- A theorem prover for first-order linear logic.
- An implementation of the LolliMon logic programming language.

Both are available at the project home page at `http://www.cs.cmu.edu/~self`.